Merchant
User Guide

PIN Debit Processing

September 29, 2009 | Version 1

CHASE Paymentech

4 Northeastern Blvd.
Salem, NH 03079-1952
603.896.6000
www.chasepaymentech.com

PIN Debit Processing

A Merchant User Guide

14221 Dallas Parkway
Dallas, TX 75254

4 Northeastern Boulevard
Salem, New Hampshire 03079–1952
603.896.6000
www.chasepaymentech.com

Revision History

Date	Revision Summary	Page(s)
09/29/09	User guide title changed to *PIN Debit Processing – A Merchant User Guide*	
	PIN-Based Encryption section – Overview – added Triple DES information – Debit key management – added sub-bullet under Injection of Encryption Keys	4
	Adjustments/Chargeback Processing – Overview – added information on representments	10
	Network Characteristics descriptions updated	11 - 13

Table of Contents

Debit Processing

Overview

Point-of-sale (POS) debit processing allows consumers to use their Automated Teller Machine (ATM)/Debit cards to access funds in their checking accounts to pay for goods and services. There are currently two types of POS debit transactions:

- PIN-based, or on-line debit
- Signature-based, or offline debit

PIN-based (On-Line Debit)

Overview

Online debit cards require electronic authorization of every transaction and the debits are reflected in the user's account immediately. The transaction is secured with the personal identification number (PIN) authentication system.

PIN-based debit is generally viewed as superior to signature-based debit because of its more secure authentication system and live status, which alleviates problems with processing lag on transactions that may have been forgotten or not authorized by the owner of the card.

Benefits of accepting PIN debit

Reduced Interchange

A PIN debit transaction processed over a debit network will come with different transaction costs and interchange compared to a debit transaction processed as a signature transaction over the VISA or MasterCard network.

Currently, the Interchange costs associated with the debit networks are lower than most other electronic payment alternatives. The associated merchant costs may vary depending on the merchant type and average ticket. Compared to credit transactions, however, the interchange for both PIN-based and signature debit transactions is typically lower. Please contact your Chase Paymentech representative to request the current PIN debit rates that apply to your industry.

Guaranteed Payment

When an approval is received on a PIN debit authorization request, the funds are immediately withdrawn from the consumer's bank account thus providing virtually guaranteed funds to the retailer.

Consumer Demand

Many consumers like the convenience of PIN-based transactions because of the added security and speed at the Point of Sale. Additionally, the ability to receive "cash-back" with a PIN debit purchase is an added benefit.

Merchant requirements

To offer the PIN-based debit payment option to consumers via any of the eleven U.S. debit networks, merchants must be based in the United States.

Canadian-based merchants can process transactions through Interac and Maestro PIN debit.

Support

PIN-based debit transactions are supported in a retail environment on the Chase Paymentech host.

Continued on next page

PIN-Based (On-Line Debit), Continued

Cash back	The Cash back feature allows a cardholder the option of receiving additional cash over the amount of the original purchase. Once the data is collected, Chase Paymentech sends the information to the networks in a separate field. A merchant is not required to offer cash back.
Debit surcharges	Please check with your Chase Paymentech representative regarding the ability to surcharge PIN debit since the rules and restrictions vary depending on the debit network.
Store and forward	A Store and Forward (SAF) transaction is a POS transaction that has been authorized by the merchant in an offline mode, is stored in the merchant's system electronically and is retransmitted when technical problems have been resolved. Each SAF transaction is performed at the sole risk of the merchant who bears all liability for non-payment of goods and services dispensed in connection with such transactions.

PIN-based Encryption

Overview

Encryption is the process of transforming clear or plaintext into ciphertext for security or privacy. Encryption is the intentional scrambling or masking of digital data to protect it from compromise.

Data Encryption Standard (DES) utilizes symmetric-key (or private-key) encryption, in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The key is a string of digits that has been generated by a complex mathematical algorithm, or formula.

Triple DES (**TDEA/TDES/3DES,** or Triple DEA) is the process that uses 2 (or 3) keys instead of one. In this process the data to be encrypted; e.g. PIN, is first encrypted under one key (K1), the result is decrypted under another key (K2) and then the result gets encrypted again under either the first key (K1) or a third key (K3). There are 3 cryptographic functions in this process; hence it is called Triple DES. Triple DES is now a mandatory requirement in ANSI Standards (X9.8 Part 1 and X9.24 Part 1).

A PIN Block is created by combining the Personal Account Number (PAN) with the Personal Identification Number (PIN). This number is combined with a Data Encryption Key and processed through an algorithm. This process is called encryption and is intended to transform the original number into another series of numbers that will be passed on from the POS device to the Host Security Module (HSM).

Debit key management

Following the rules below will help to ensure proper debit key management

- PIN Entry Devices (PEDs) must have TDES encryption keys loaded (injected)
- A Base Derivation Key (BDK) is the type of encryption key injected into PIN pads
  - This key ensures PINs are encrypted when communicating from PIN pad to host
  - Required for both functionality and security
- Injection of encryption keys is industry regulated and **must** be secure
  - ANC X9.8, TR-39 (TG-3), The TR-39 is a PIN Security guideline which is intended to be used to implement a uniform security review for all entities which handle PINs and/or cryptographic keys used to secure PINs. Any entity which plans to share keys with Chase Paymentech must complete and submit a TR-39 review prior to sharing keys
- It is paramount that these keys not be compromised at any time during their life cycle
  - Key compromises will result in immediate destruction of the merchant's key and their ability to process debit

Continued on next page

PIN-based Encryption, Continued

Debit key management, continued

- Two methods of encryption currently supported by Chase Paymentech:
  - Single DES DUKPT
    - This method is being phased out, no new key creations as of 4/1/07
  - Triple DES DUKPT
    - Triple DES (TDES or 3DES), began using this method in February of 2007.

According to VISA mandate, all merchants must be converted to TDES by 7/1/10.

PIN entry devices

PIN entry devices and their compliant firmware used must be listed on the VISA approved PIN Entry Device List. This list is published at www.visa.com/pin. Directions to register a PIN entry device not currently listed may also be found on the website.

For debit card processing, any PIN pad deployed after 7/1/07 must be triple DES capable. For more information regarding triple DES requirements, refer to www.visa.com/pin.

Host Security Module (HSM)

Many big box merchants have configured an HSM to process debit transactions with Chase Paymentech. Instead of utilizing a BDK for each terminal to the Chase Paymentech Host, the BDK is used to communicate between the terminal and the merchant's host system. The merchant's host then communicates via a Zone Master Key (ZMK) to the Chase Paymentech Host.

Things to keep in mind:

- A Zone Master Key (ZMK) is shared between the merchant's host and the Chase Paymentech host. This is a key which enables the merchant's host to send transactions with encrypted PINs through to the Chase Paymentech host.
- The BDK that is used to inject the merchant's PIN pads is loaded only on the merchant's host and is not shared with Chase Paymentech. It is up to the merchant's host system to manage any key exchanges between terminal and the merchant's host system.
- Merchants with an HSM must go through the same due diligence to ensure they are compliant, because they are sharing a ZMK key with Chase Paymentech.

Continued on next page

PIN-based Encryption, Continued

Key creation setup

A Base Derivation Key (BDK) is created as a Triple DES. Once this key BDK has been created, it will be set up under the unique client/division established on the Host. The new BDK will be sent to a certified Encryption Service Organization (ESO) upon request to be injected into merchant PIN pads

ESO Certification requirements

The following are Chase Paymentech certification requirements for all ESOs doing PIN pad key injections:

- Must complete and sign the Chase Paymentech Security Agreement
- Must submit TG-3 audit and Interlink Self Audit every two years
- Must complete debit network registration (STAR, NYCE, Interlink, & ACCEL) paperwork
- Must pay applicable network registration and annual fees
- Must comply with an On-site visit by a Chase Paymentech Compliance Representative

Signature-based (Off-Line Debit)

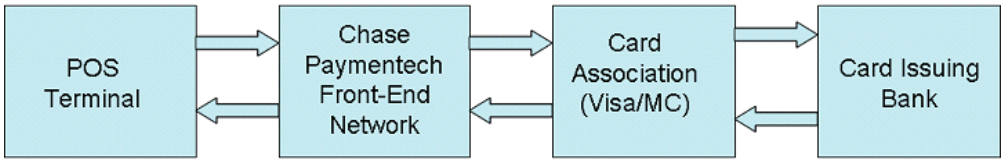
Overview

Signature-based debit transactions are inaccurately referred to as “credit” transactions even though no credit is actually involved. This is because they are processed through the Visa or MasterCard networks in the same manner as actual credit card transactions. Since they are handled like any other Visa or MasterCard transaction, U.S. offline debit cards are also accepted worldwide at virtually all merchants that accept credit cards of the corresponding brand, even if they do not accept their own country’s debit cards.

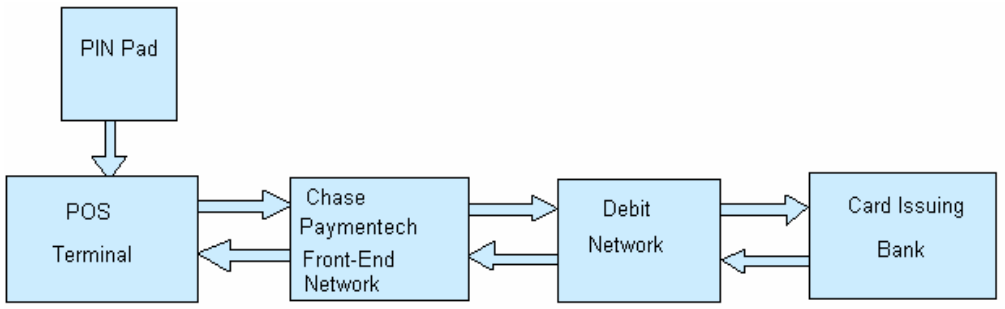
Offline debit cards have the logos of the major credit cards (i.e., Visa or MasterCard). They are used at the POS like a credit card. Transactions are referred to as Off Line because it typically takes two to three days for the transaction to post to the cardholder account

Debit Transaction Flows

Signature-based transaction flow

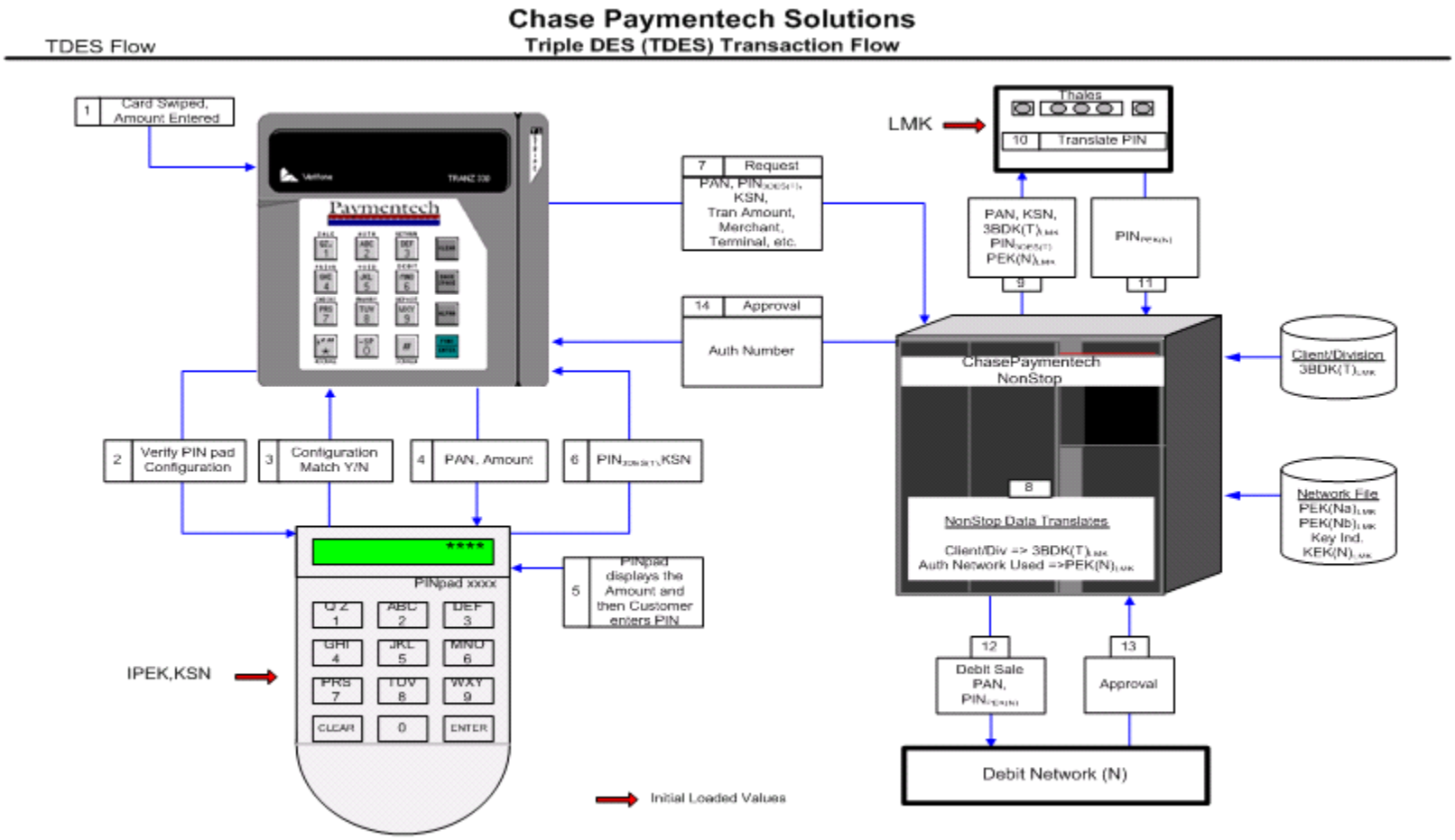


PIN-based transaction flow



Continued on next page

Debit Transaction Flows, Continued



The designation (T) means "of the terminal" and (N) means "of the network" (i.e. $PIN_{3DES(T)}$ means the PIN encrypted under the Triple DES key of the terminal).

Adjustment/Chargeback Processing

Overview

An ***adjustment*** occurs when a merchant disputes a debit card transaction with an acquirer. The acquirer initiates an adjustment against the cardholder's account. For example, if a cardholder receives goods from a merchant, but the merchant does not get paid for these goods, an adjustment request is communicated to the acquirer. The acquirer creates an adjustment to the debit network to debit the cardholder's account (take money away) and credit (give money) the merchant's account.

Adjustments are initiated via a web-based system provided by each individual network. The adjustment process is manual and does not generate a real time transaction response. In general the debit or credit to the consumer account occurs within 3 to 5 days but it may take up to 30 days for the network to respond.

A ***chargeback*** occurs when a card holder disputes a debit card transaction with his or her issuer. The card issuer initiates a chargeback against the merchant account. For example, if a cardholder is charged twice for an item they contact their bank/issuer. The issuer sends a chargeback to the debit network. The issuer credits the cardholder (give money) and forwards the chargeback to the acquirer via the debit network to debit the merchant (take money away).

A ***representment*** is the attempted reversal of a chargeback by a merchant or acquirer to the issuing bank of the chargeback with the required documentation to support the reversal request.

Adjustments are generally initiated by the merchant/acquirer and chargebacks by the cardholder/issuer. Both an adjustment and chargeback can be a credit or debit to the cardholder's account.

Network Characteristics

ACCEL

ACCEL/Exchange is owned and operated by Fiserv EFT. ACCEL/Exchange is available in all 50 states. ACCEL is one of the four networks that supports PINless debit.

All Chase Paymentech EBT transactions are processed by ACCEL.

AFFN

AFFN was founded in 1985 at the request of the U.S. Army in support of the "Surepay" direct deposit system, to provide U.S. military personnel (active, reserve, dependents, and retired) with access to their funds through ATM and point-of-sale terminals at or near U.S. military bases worldwide.

Alaska Option

There is no direct connect to Alaska Option. Authorizations are sent to Fifth Third and a gateway fee applies.

The predominance of Alaska Option issued cards is within the state of Alaska.

CU24

The Credit Union 24® Network was created in 1981 by four Central Florida credit unions. Credit Union 24 Network Participants are located throughout the United States.

Continued on next page

Network Characteristics, Continued

Interlink

Interlink, which is owned by Visa, is America's leading online point-of-sale network**.** Interlink has merchant locations in every state. The majority of PIN debit transactions in the U.S. today are processed through Interlink.

Jeanie

Jeanie is the network brand owned by Fifth Third and is predominantly issued in the Mid West.

Maestro

Maestro, which is owned by MasterCard, is a PIN-based, global, direct cash access. Maestro card acceptance and cash access at merchants and ATMs is available in more than 93 countries around the globe.

NYCE

NYCE is owned by Metavante and was originally formed by the five largest banks in New York. This network is national in coverage and also one of the four networks that supports PINless debit transactions.

PULSE

PULSE is a wholly owned Discover Financial Services, Inc. company since January 2005. PULSE was organized in December 1980 and incorporated on July 29, 1981. The network was founded and initially funded by seven of the ten largest bank holding companies in Texas. PULSE is one of the four networks that supports PINless transactions.

Network Characteristics, Continued

SHAZAM

SHAZAM started as an ACH processor for the state of Iowa and has evolved to offer debit services to merchants and cardholders nation wide. The majority of cards are issued within the states surrounding Iowa.

STAR

STAR Networks Inc., a First Data company, is one of America's leading PIN-secured debit networks. Star is one of the four networks that support PINless debit transactions.

Interac

Chase Paymentech supports the Canadian debit network – Interac. Interac Association is the organization responsible for the development and operation of a national network of Interac Direct Payment (IDP), Canada's national debit service. In addition to offering PIN debit services, Interac also offers Interac ON Line for ecommerce purchases.

Reconciliation

Overview

Both summary and detail reports are available to assist in balancing your internal records with the activity recorded by Chase Paymentech. These reports are available on line or may be obtained electronically via FTP. Please review the Merchant Reporting Guide provided on Paymentech Online for lists of available reports, instructions on how to access reports and samples of selected reports.

Reports available

The **Deposit Activity Summary Report (FIN-0010)** contains activity, financial, fees and adjustment and funds transfer summaries for all payment types. Within this report is the transaction count and dollar amount for Debit Authorizations and Debit Deposits. The report further breaks down the Sales and Refund Count and dollar amount for each debit network.

The **Deposit Detail Report (ACT-0010)** contains transaction level detail for all deposited transactions. This report allows the user to further drill down to the method of payment (MOP) and the requested action for the transaction. Hence the report could provide the number of deposited transactions and the related amounts for each transaction approved by any one of the debit networks.

The **Service Charge Detail Report (FIN-011)** details interchange and fee assessments and Chase Paymentech fees for all payment types. This report provides the interchange per network and any related fees, such as a switch fee or an adjustment fee per network.

The **Authorization Detail Report (ACT-0036)** contains transaction level detail for all authorization requests. This report allows the user to further drill down to the MOP level.

The **Debit Adjustment Summary Report (PDE-0036)** lists debit adjustments made to previously processed and previously settled debit transactions.

Transaction history

Transaction History (TH), available on Paymentech Online, provides detail for debit adjustments that were denied by the networks. TH also provides adjustment details for previously processed debit transactions that the merchant did not deposit and therefore were not settled.

GLOSSARY

3DES	Three Key Triple Data Encryption Standard (DES)
Adjustment	Debit adjustments are an exception item initiated by a merchant or by an issuing bank to correct an error in the processing of a previous debit transaction
ANC	American Standards Committee
ANSI	American National Standards Institute
Base Derivation Key (BDK)	A derivation key normally associated with Derived Unique Key Per Transaction
Big Box Merchant	A physically large chain store often referred to as super store, mega store or super center.
Ciphertext	The encrypted text of a message, which may be decrypted back to clear text only by someone who has the correct Key.
Decryption	A process of transforming ciphertext back into cleartext. Synonym for decipherment.
DES	Data Encryption Standard. A commonly used synonym for DES, derived from a Federal Information Processing Standard Publication (FIPS Pub. 46, “Data Encryption Standard” algorithm). Intended to protect sensitive data.
DUKPT	Derived Unique Key per Transaction – a key management method which uses a unique key for each transaction, and prevents the disclosure of any past key used by the transaction –originating TRSM. The unique Transaction keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.
Encryption	The mathematics process whereby data is scrambled for security reasons. A process of transforming plaintext into ciphertext for security or privacy.
ESO	Encryption Service Organization; a third party that offers key loading into PIN pads
HSM	Host Security Module; A TRSM device used to translate PINs, PIN block formats, keys and create cryptograms of keys stored in application databases.
IPEK	Initial PIN Encrypting Key
KEK	Key Encrypting Key
Key	Also Cryptographic key. A mathematical value that is used in an algorithm to transform plaintext into ciphertext or vice versa. A password or file needed to decipher encrypted data.
Key loading	The process of loading a key into TRSM

Continued on next page

GLOSSARY, Continued

Key management	The activities involving the handling of cryptographic keys during the entire life cycle of the keys.
Key management procedures	A document or set of documentation that describes in detail the organizational structure, responsible roles, and organization rules for the functions identified in the key management policy and demonstrated by the use of a series of steps followed in a regular, definite order.
KSN	Key Sequence (serial) Number
LMK	Local Master Key; the master key which typically resides inside the HSM
PEK	PIN Encryption Key
Personal Identification Number (PIN)	The code or password the customer possesses for verification of identity.
PIN block	A 64-bit block of data formed by combining PIN and PAN numbers which will be (TDEA) enciphered in such a way as to insure that the encipherment of a plaintext PIN value using a particular cryptographic key does not predictably produce the same enciphered value when the same PIN value is associated with the different accounts.
PIN entry device (PED)	The device into which the cardholder inputs the PIN. **Note:** A PIN entry device may also be referred to as a PIN pad, EPP, SPED, TREPP, etc.
TRSM	Tamper Resistant Security Module; a physically secure device that is qualified to perform cryptographic functions
ZMK	Zone Master Key